Patent
Atty Docket No. 156906-0008

AMENDMENTS TO THE SPECIFICATION

Please add the following new paragraphs to the Specification:

[0029A] FIG. 13 is a diagram of a security module for authenticating and verifying data cards when first inserted in a reader and, potentially with transactions thereafter.

[0029B] FIG. 14 is a process flow chart of a preferred cross-authentication procedure as may be carried out between a card reader and a security module.

[0029C] FIG. 15 is a conceptual diagram illustrating various interfaces among components of the cashless portion of a combined bill acceptor and card reader system, with application to an electronic gaming machine as the host device.

[0029D] FIG. 16 is a flow chart diagram illustrating the operation of a gaming system in accordance with a preferred embodiment as described herein.

Please amend paragraphs [0061], [0062] and [0064] of the specification as follows:

[0061] In one or more embodiments as disclosed herein, the combined bill acceptor and card reader 201 may also comprise, or interface with, a special security module which authenticates and verifies cards 250 when first inserted in the smart card reader 211 and, potentially, in connection with each cashless transaction thereafter until the card 250 is removed. A preferred embodiment of a security module 1300 for such a purpose is illustrated in Fig. **[[3]]** 13. As shown in Fig. **[[3]]** 13, the security module **[[300]]** 1300 comprises a first interface **[[313]]** 1313 (such as an RS-232 serial

communication port), which is connected to the combined bill acceptor and card reader 201, a microprocessor **[[310]]** 1310, a memory **[[314]]** 1314 (which is divided into data memory **[[320]]** 1320 and program memory **[[321]]** 1321), and a second communication interface **[[312]]** 1312 (such as an RS-232 serial communication port), which is connected to the game device processor. Two communication port managers **[[311]]** 1311, **[[315]]** 1315 (each of which may take the form of a universal asynchronous transceiver/receiver (UART)) are resident with the microprocessor **[[310]]** 1310, for handling communications over the communication interfaces **[[312]]** 1312 and **[[313]]** 1313, respectively. Alternatively, the communication port managers (e.g., UARTs) **[[311]]** 1311, **[[315]]** 1315 may be located off-chip from the microprocessor **[[310]]** 1310.

[0062] In a preferred embodiment, the microprocessor **[[310]]** 1310 of the security module **[[300]]** 1300 is programmed to, among other things, perform one side of a cross-authentication check when a gaming session starts, and periodically thereafter. Programming instructions for its part of the cross-authentication check are stored in program memory **[[321]]** 1321. Likewise, programming instructions for the counterpart of the cross-authentication check conducted by the combined bill acceptor and card reader 201 are stored in the program memory (EEPROM 215 or RAM 216) of the card reader 202.

[0064] Fig. 14 is a process flow chart of a preferred cross-authentication procedure as may be carried out between a card reader (e.g., card reader 202 shown in

FIG. 2 or card reader 1505 shown in FIG. 15) and the security module (e.g., security module **[[300]]** 1300 shown in FIG. **[[3]]** 13 or security module 1510 shown in FIG. 15), or between the card reader 202 or 1505 and a portable data device (e.g., a smart card). For convenience, the following explanation will be presented in the context of the system 1500 depicted in FIG. 15. As illustrated in Fig. 14, in a first step 1401, a random number R1 is generated by the card reader 1505. In a next step 1402, the random number R1 is enciphered by the card reader 1505 using a common key (which may be stored in SAM 217), yielding enciphered random number R1'. Concurrently, in step 1420, a random number R2 is generated by the security module 1510, and in a following step 1421, the random number R2 is enciphered by the security module 1510 using the same common key, yielding enciphered random number R2'. The enciphered random numbers R1', R2' are then exchanged by the card reader 1505 and the security module 1510. In step 1403, the card reader 1505 deciphers enciphered random number R2' using the common key, thus obtaining the original random number R2, and generates a session key S from R1 and R2 in step 1404. Likewise, in step 1422, the security module 1510 deciphers enciphered random number R1' using the common key, thus obtaining the original random number R1, and generates the same session key S from R1 and R2 in step 1423, using the same algorithm to do so as the card reader 1505.